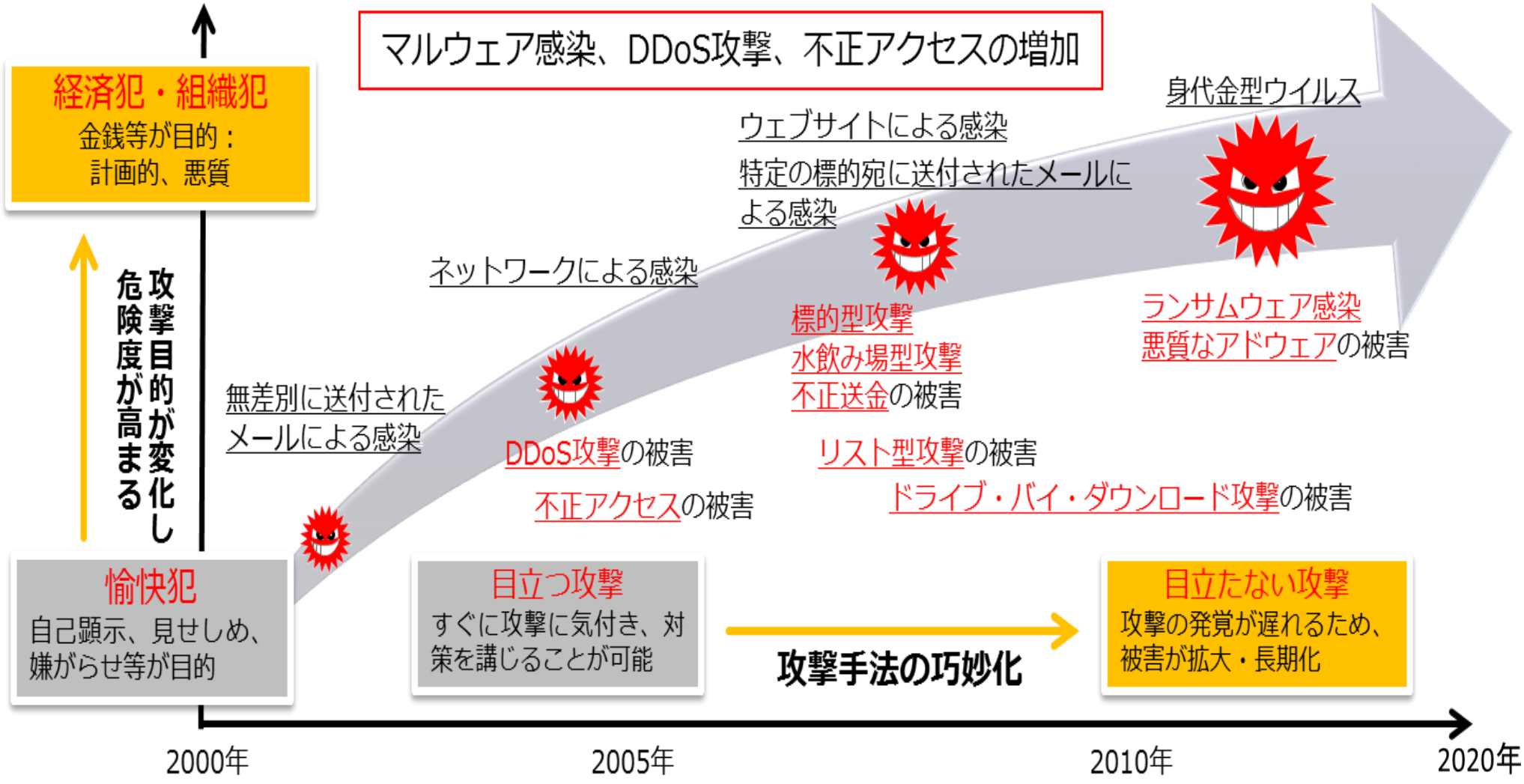
資料27－１

サイバー攻撃の最近の動向等について

サイバーセキュリティタスクフォース事務局

令和2年 12月3日

サイバーセキュリティ上の脅威の増大



OSの脆弱性を利用した攻撃（⇒ワームの大規模感染） → **IoTへの攻撃**

昨今のサイバー攻撃の事例

国内事例

出典：各種公開資料等より総務省作成

2015年６月	日本年金機構の職員が利用する端末がマルウェアに感染し、年金加入者の情報約125万件が流出（標的型攻撃）
2015年11月	東京五輪組織委員会のホームページにサイバー攻撃、約12時間閲覧不能（DDoS攻撃）
2016年６月	i.JTB（JTBのグループ会社）の職員が利用する端末が、マルウェアに感染し、パスポート番号を含む個人情報が流出した可能性（標的型攻撃）
2017年５月	国内（行政、民間企業、病院等）において、WannaCryによる被害が確認。企業内のシステム停止などの障害が発生（ランサムウェア）
2018年１月	コインチェック社が保有していた暗号資産（仮想通貨）が外部へ送信され、顧客資産が流出（不正アクセス）
2020年	**三菱電機やNEC等において防衛関連情報を含む情報が外部へ流出した可能性が判明（不正アクセス）** **ドコモ口座経由で、不正に入手された口座番号・暗証番号等を使用した不正出金が判明（不正アクセス）** **カプコンがランサムウェアによる標的型攻撃を受け、個人情報等が外部へ流出した可能性が判明（ランサムウェア）**

海外事例

2015年６月	米国の人事管理局（OPM）が不正にアクセスされ、政府職員の個人情報が流出（不正アクセス）
2015年12月	ウクライナの電力会社のシステムがマルウェアに感染し、停電が発生（標的型攻撃）
2016年10月	米国のDyn社のDNSサーバが大規模なDDoS攻撃を受け、同社のDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生（DDoS攻撃）
2017年５月	世界各国（アメリカ、イギリス、中国、ロシア等）でWannaCryの感染被害が発生。行政、民間企業、医療等の多くの組織に影響（ランサムウェア）
2017年10月	米Yahoo社で約30億件の個人情報が流出していたことが判明（不正アクセス）
2019年９月	エクアドルで国民ほぼ全員を含む約2000万人分の個人情報が海外に流出（不正アクセス）

その他、最近では、新型コロナウィルスに乗じたサイバー攻撃の事例を多数確認

サイバー攻撃の脅威の増加

➢ 新型コロナへの対応として、テレワークの普及拡大や社会全体のデジタル・トランスフォーメーション（DX）が進みつつある中、サイバー攻撃も増加。

４月　国内高校の半数が利用するClassi社が**不正アクセス**を受け、**IDや暗号化パスワード等が流出**した可能性が判明。

５月　NTTコミュニケーションズ従業員の**テレワーク環境(仮想デスクトップ)に係るアカウント及びパスワードが窃取**され、**顧客情報（防衛省等の政府機関を含む）が流出**した可能性が判明。

６月　ホンダが**サイバー攻撃**を受け、**世界の９工場で生産を一時停止**。

７月　Twitter社で**ソーシャルエンジニアリング**により社内ツールが不正利用され、詐欺投稿が行われ、**データも流出**した可能性が判明。

８月　国内数十社において、**VPN機器の脆弱性を悪用した不正アクセス**が行われVPN接続用のパスワードなどが流出した可能性が判明。

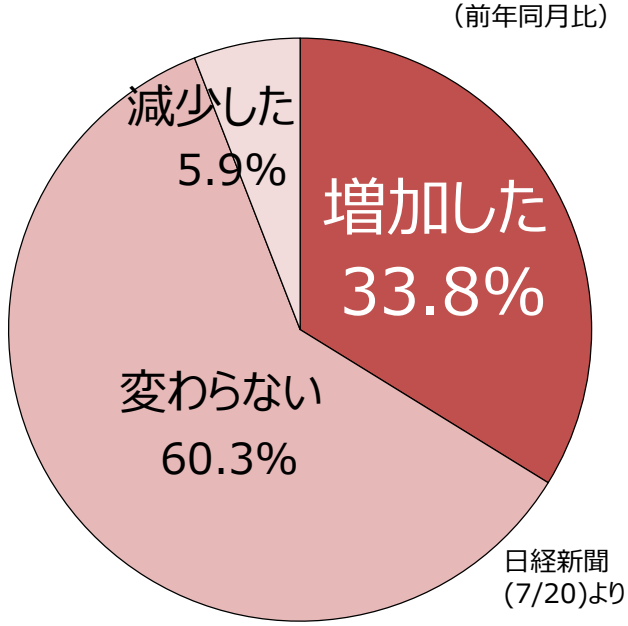
９月　ドコモ口座が悪用され、第三者が**不正に入手した口座番号、暗証番号等を使用**した口座振替による**不正出金**が判明。

10月　原子力規制委員会が、**不正アクセス**を受け、メール等のやりとりを含む**外部とのアクセスを遮断**。

11月　カプコンが、**オーダーメイド型ランサムウェアによる標的型攻撃**を受け、**個人情報・人事情報・開発資料等が流出**した可能性が判明。

（piyolog、各社公表資料、各種報道等より総務省作成）

2020年４月以降に受けたサイバー攻撃

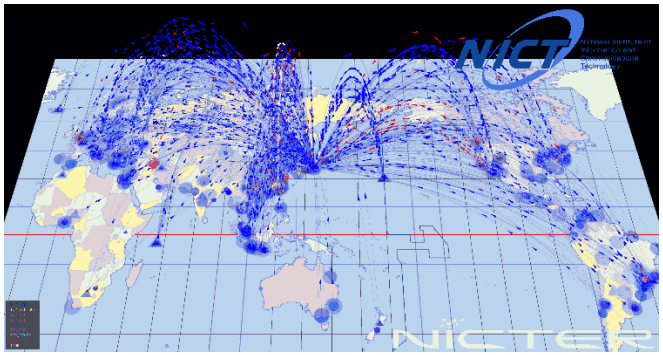


社内システム・設備の停止や提供しているサービスの停止といった企業活動そのものに影響する攻撃が増加

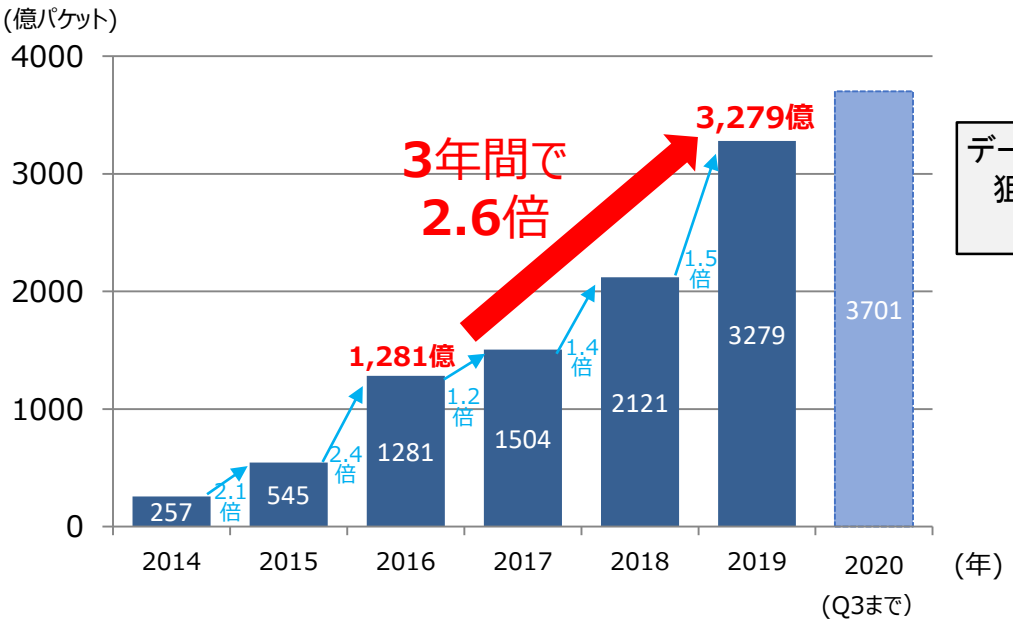
IoT機器を狙った攻撃

■ IoT機器を狙った攻撃は依然として多い。

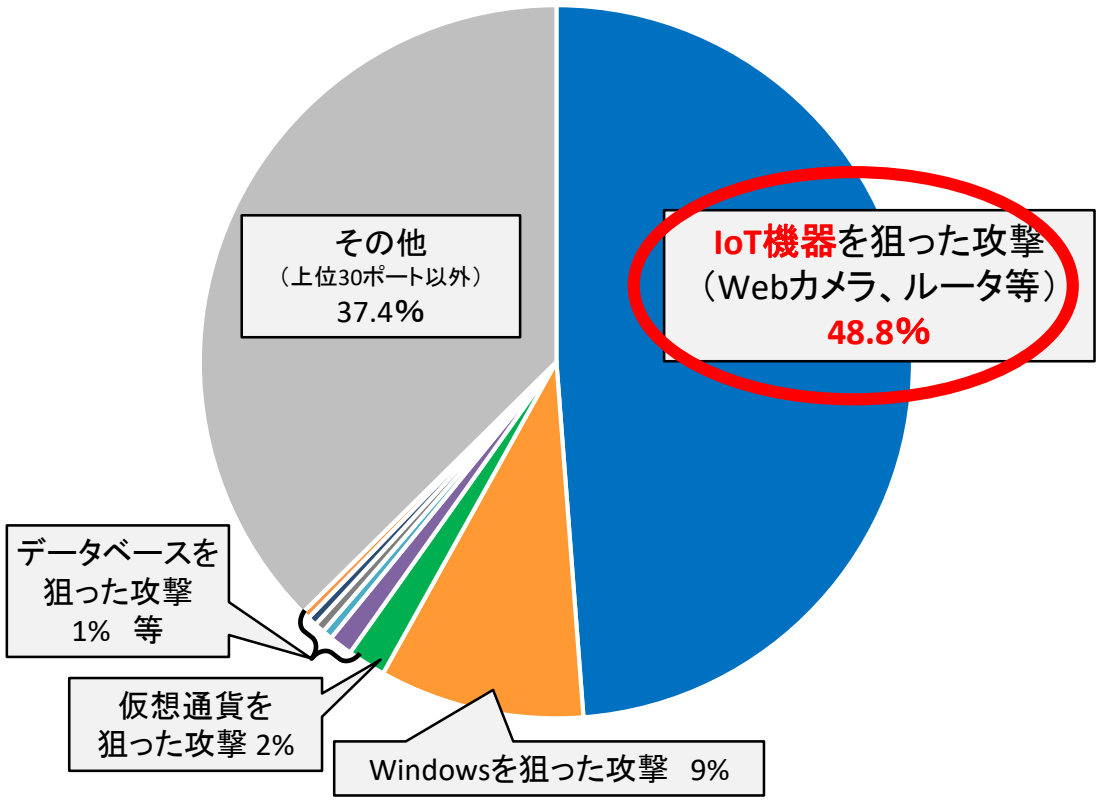
NICTERにより観測されるサイバー攻撃の様子



NICTERで１年間に観測されたサイバー攻撃回数



約半数がIoT機器を狙った攻撃



※ NICTERで2019年に観測されたパケットのうち、調査目的パケット以外についてサービス種類（ポート番号）ごとに上位30ポートまでを分析したもの。

※ IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

IoT機器調査及び利用者への注意喚起結果（2020年10月度）

- 参加手続きが完了しているISP（インターネット・サービス・プロバイダ）は**64社**。
  当該ISPの**約1.1億IPアドレス**に対して調査を実施。
- **NOTICE**による注意喚起は、**１，８５２件**の**対象を検知**しISPへ通知。
- **NICTER**による注意喚起は、１日平均**１３８件**の**対象を検知**しISPへ通知。

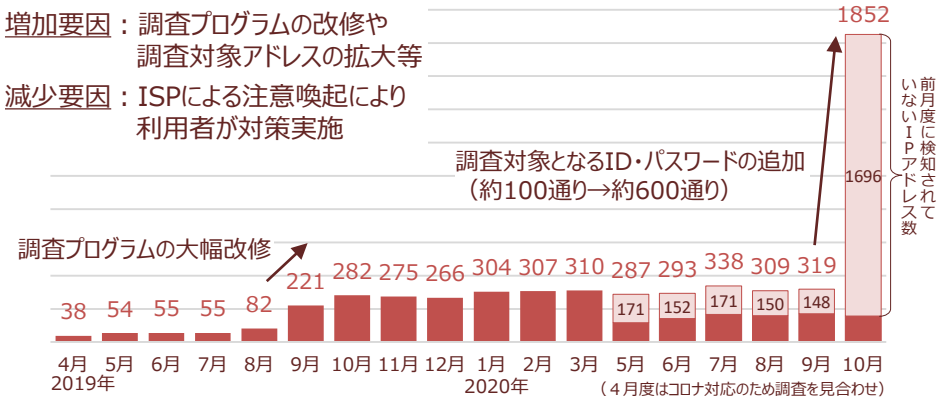
NOTICE注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

1,852件（9月度:319件）

（参考）　2020年度の累積件数：3,398件（2019年度：2,249件）
ID・パスワードが入力可能だったもの：6.0万件

*) 特定のID・パスワードによりログインできるかという調査をおおむね月に1回実施し、ログインでき、注意喚起対象となったもの（ユニークIPアドレス数）



NICTER注意喚起※の取組結果

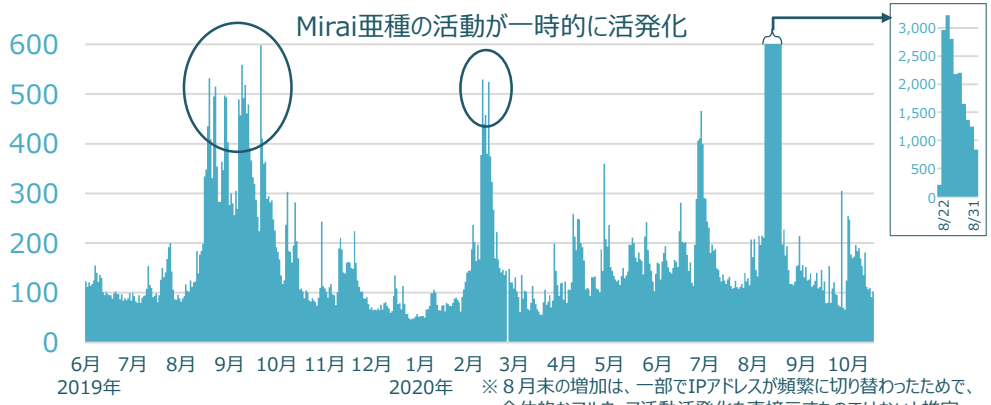
※マルウェアに感染しているIoT機器の利用者への注意喚起

注意喚起対象としてISPへ通知したもの**

１日平均138件（9月度:186件）

（参考）　期間全体での値：1日平均196件
最小：46件(2020/1/9)／最大：3,227件(2020/8/24)

**) NICTERプロジェクトによりマルウェアに感染していることが検知され、注意喚起対象となったもの（ユニークIPアドレス数）



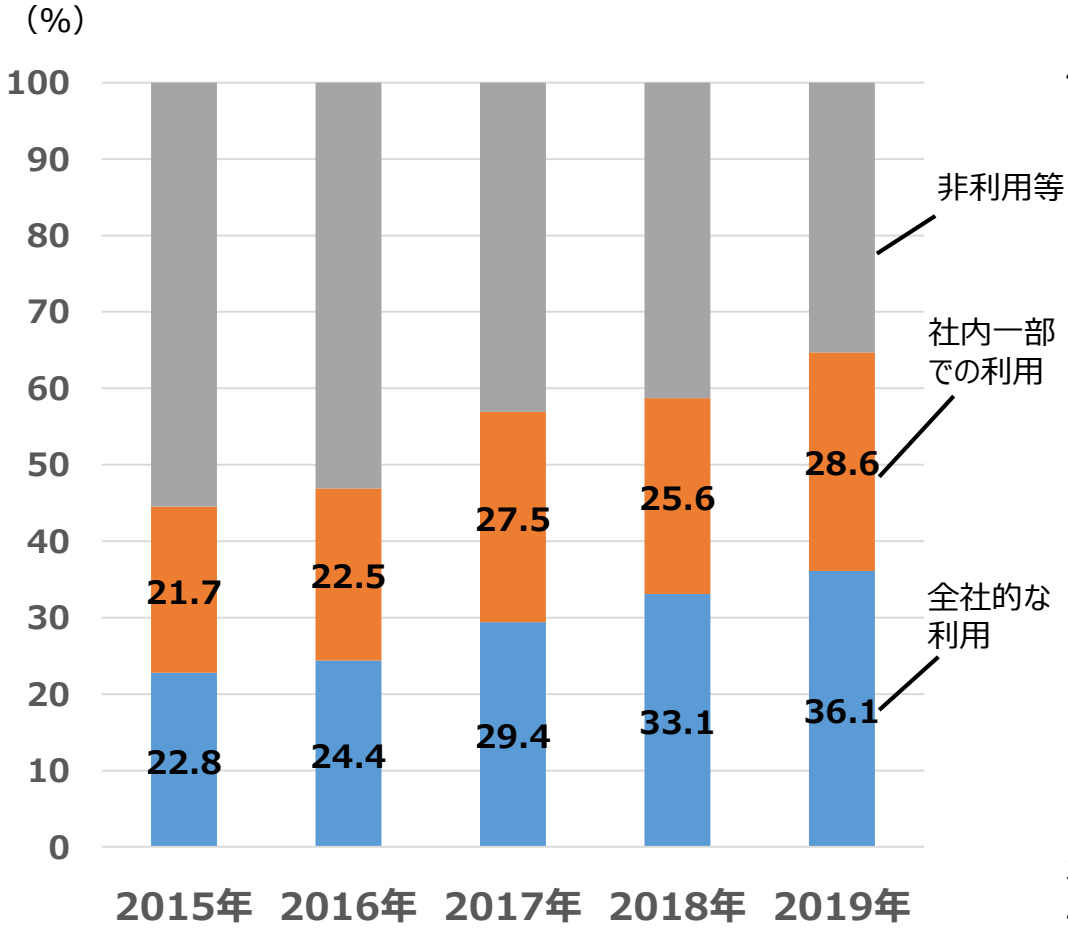
※８月末の増加は、一部でIPアドレスが頻繁に切り替わったためで、全体的なマルウェア活動活発化を直接示すものではないと推定
参考：https://blog.nicter.jp/2020/10/jp_mirai_spike/

NOTICE注意喚起については、通知件数が大幅に増加していますが、これは、2020年10月度から調査するID・パスワードを追加（約100通り→約600通り）した結果増加したものです。なお、NICTER注意喚起については、2020年10月度分については、全体として大きな変化はありません。

クラウドサービスの利用の拡大とセキュリティ

■ 民間企業におけるクラウドサービスの利用率は年々拡大している一方で、サービスの可用性の確保といったセキュリティ対策の重要性が増している。

クラウドサービスの利用状況



出典：令和2年版　情報通信白書

クラウドサービスの停止事故

例）Amazon Web Service（AWS）における障害（2019年8月）

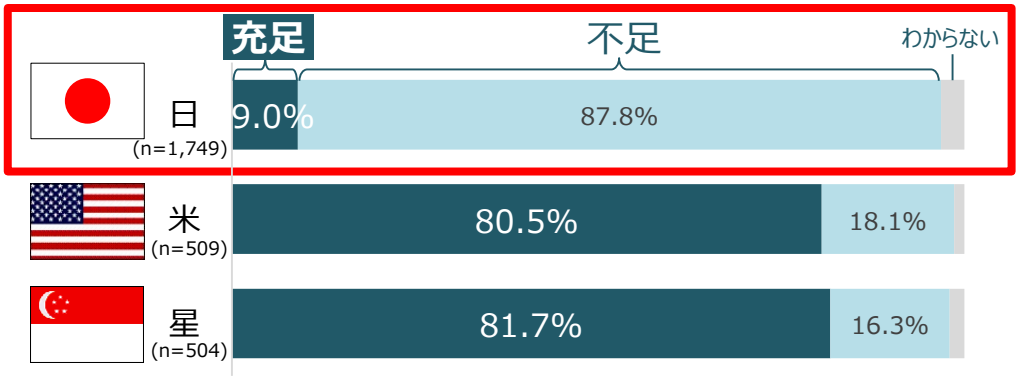
- AWSの東京リージョンの１つのアベイラビリティゾーン（AZ）において、空調設備の管理システムの障害が原因でサービス障害が発生。
- 原因はサードパーティ製の制御システムにおけるバグとフェイルセーフとして用意されていたパージモードの動作不良。
- 最終的な回復まで７～８時間を要し、同サービスを利用していた、決済、SNS、社内システム、ニュース・メディア、バイクシェアなど広範囲にわたる様々なサービスが一時的に停止した。

社会全体にクラウドサービスが普及するにつれ、クラウドサービスの可用性を含むセキュリティの確保が重要な課題となっている。

セキュリティ人材の不足

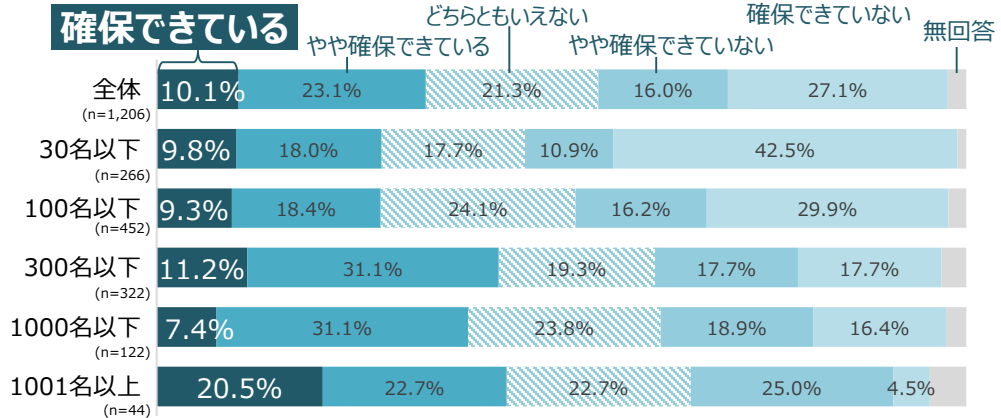
- 日本では人材の不足感が高く、セキュリティ人材が充足していると感じている企業は１割程度。
- ＩＴ企業においても、セキュリティ人材を「確保できている」との回答は１割に留まる。
- 各企業のセキュリティ対策としても人材育成は喫緊の課題。

セキュリティ対策に従事する人材の充足状況



出典：NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2019」より作成

IT企業のセキュリティ専門技術者の確保状況



出典：IPA「IT人材白書2019」より作成

今後の投資を要するセキュリティ対策

(n=313)

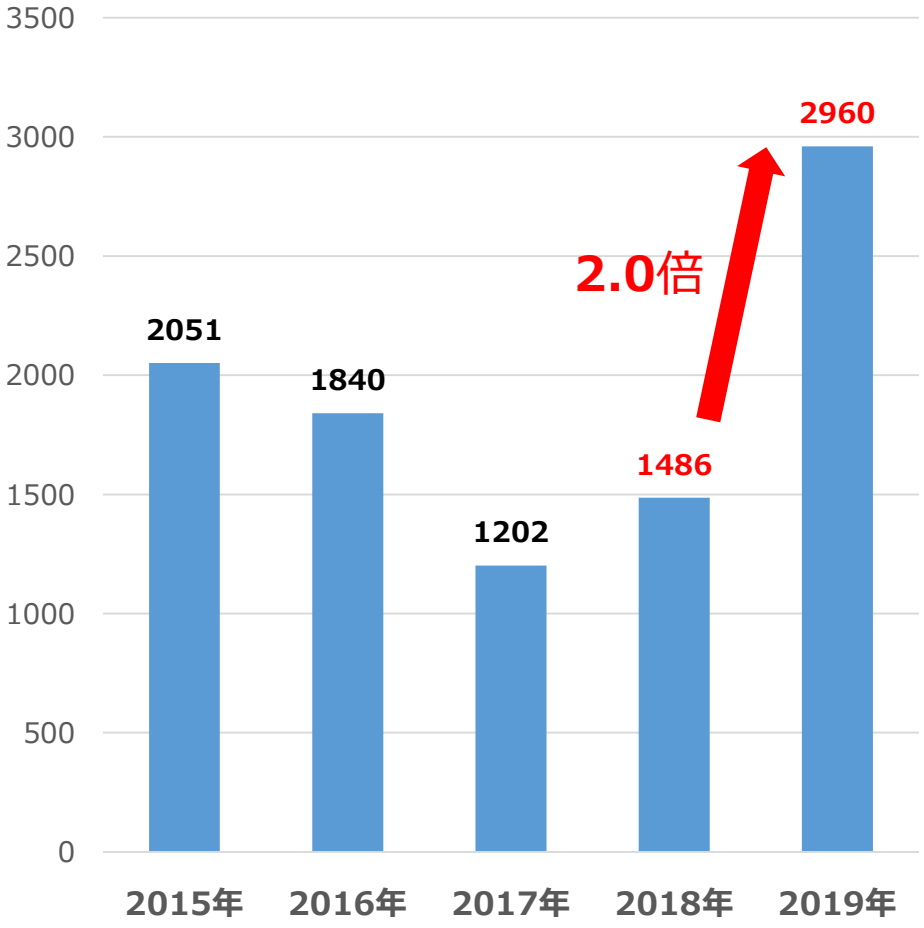
サイバーセキュリティ人材の育成	**56.2%**
セキュリティ監視の強化	52.1%
内部不正対策	50.5%
IoT／クラウド環境におけるセキュリティ対策	49.5%
インシデント対応体制（CSIRT）の強化	43.5%
モバイルデバイスの保護	43.1%
マルウェアやランサムウェア対策	40.6%
事業継続管理	39.3%
サイバーセキュリティ経営体制の構築	32.3%
脆弱性診断やペネトレーションテスト	30.0%
Webサイトやインターネット公開システムの保護	24.9%
外部委託先管理	24.6%
制御システム環境におけるセキュリティ対策	22.0%
プリバシー情報の保護	17.9%
ブロックチェーン／仮想通貨の利用環境におけるセキュリティ対策	4.5%
その他	1.9%
特にない	1.3%

出典：KPMGコンサルティング・EMCジャパンRSA「サイバーセキュリティサーベイ2019」より作成

不正アクセス行為等の発生状況

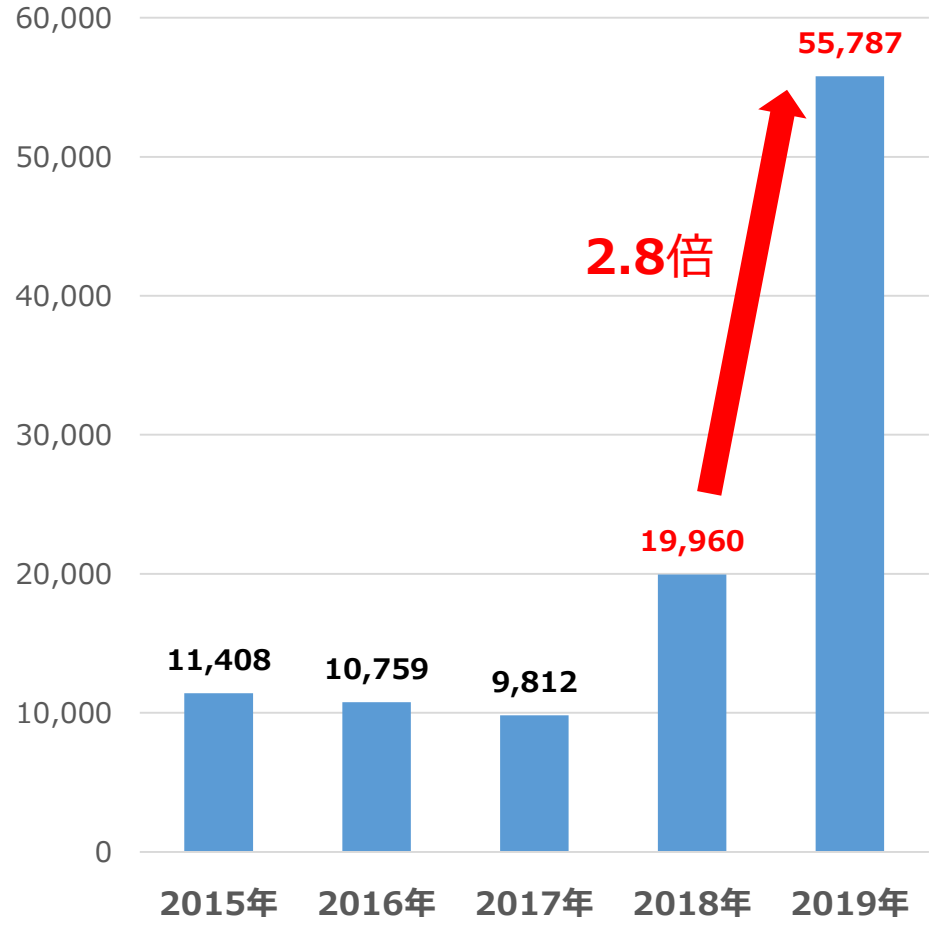
■ 不正アクセス行為の認知件数及びフィッシング届出件数のいずれも増加している。

不正アクセス行為の認知件数



出典：「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」（令和２年３月警察庁・総務省・経済産業省）

フィッシング届出件数



出典：「フィッシングレポート2016」~「フィッシングレポート2020」（フィッシング対策協議会技術・制度検討WG）

参考資料
（関連する主な取組）

IoT・5Gセキュリティ総合対策2020（2020年7月公表） 全体概要

■ サイバーセキュリティタスクフォースにおけるこれまでの短期的・中長期的な観点の議論、「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項 [緊急提言]」※1の内容、さらには新型コロナウイルス感染症への対応等を踏まえつつ、「IoT・5Gセキュリティ総合対策」※2について、必要な改定を行い、「IoT・5Gセキュリティ総合対策2020」として2020年７月に公表。
https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00126.html

● IoT・5Gセキュリティ総合対策2020の枠組み

重点的に対応すべき情報通信サービス・ネットワークの個別分野等に関する具体的施策

- ✓ IoT、5G、クラウドサービス、スマートシティ、テレワークシステムのセキュリティ
- ✓ トラストサービスの制度化と普及促進　など

具体的施策間でも連携

連携　連携　連携

研究開発
- ✓ 統合知的基盤
- ✓ ハードウェア脆弱性
- ✓ AI
- ✓ 暗号

など

人材育成 普及啓発
- ✓ 人材育成基盤
- ✓ サイバー演習
- ✓ 地域の人材育成

など

情報共有 情報開示
- ✓ 情報共有基盤
- ✓ 情報開示の促進

など

連携

国際連携
- ✓ ASEAN各国や欧米諸国等との連携
- ✓ 国際標準化

など

● 改定に当たっての主要な政策課題

1 COVID-19 への対応を受けたセキュリティ対策の推進

① テレワークシステムのセキュリティに関するチェックリストの作成や相談対応体制の拡充など、特に中小企業を念頭においたテレワークセキュリティの確保のための実践的な対策を推進する。

② ネット上で業務・手続を完結可能とするため、電子署名やeシールなどのトラストサービスの制度化や普及促進を図るとともに、制度・手続・慣習の見直しを進める。

2 5G の本格開始に伴うセキュリティ対策の強化

① 5Gネットワークの脆弱性及び脅威の検証・分析のための手法や体制の確立
② 関係者間のリスク・脅威情報の共有の促進
③ 規制・振興両面でのセキュリティ対策の実装の促進など

（セキュリティ・バイ・デザインの観点で推進）

3 サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

巧妙化・多様化するサイバー攻撃に対処するため、電気通信事業者における積極的なサイバーセキュリティ対策（C&Cサーバの能動的な検知や攻撃指令通信の遮断等）を迅速かつ効果的に実施可能とするため、通信の秘密の保護を図りつつ、一層のサイバーセキュリティを確保する方策について検討を行う。

4 我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

我が国におけるセキュリティ製品・サービスの海外依存や慢性的な人材不足から脱却するため、サイバーセキュリティ情報を国内で収集・蓄積(生成)・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、産学官連携の結節点とするための体制の構築を図る。

※1　2020年東京大会に向けた対処として短期的な観点から早急に取り組むべき事項を整理した結果を「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項 [緊急提言]」として 2020年１月に公表。
※2　IoT・5G時代にふさわしいサイバーセキュリティ政策の在り方について検討した結果を「IoT・5Gセキュリティ総合対策」として2019年8月に公表。

NOTICE実施計画の変更

➢ NOTICEの**実施計画**に記載された事項のうち、特定アクセス行為において**入力する識別符号**、及び特定アクセス行為の**送信元のIPアドレス**について、NICTから**変更**したい旨の申請。

→2020年９月11日付けで**総務大臣認可**　（10月度の調査から適用）

実施計画に記載が必要な事項

総務省令※において規定。

※国立研究開発法人情報通信研究機構法附則第八条第四項第一号に規定する総務省令で定める基準及び第九条に規定する業務の実施に関する計画に関する省令（平成30年総務省令第61号）第2条第2項各号

- ✓ 業務従事者の氏名・所属部署・連絡先
- ✓ 特定アクセス行為の**送信元のIPアドレス**
- ✓ 特定アクセス行為に係る識別符号の方針及び当該方針に基づき**入力する識別符号**
- ✓ 特定アクセス行為の送信先のIPアドレス範囲
- ✓ 特定アクセス行為に関する情報の適正な取扱い
- ✓ ISP等への通知先に求める情報の適正な取扱い
- ✓ その他必要な事項

変更内容

(1) 特定アクセス行為において入力する識別符号（ID・パスワード）の追加

変更前	変更後
約１００通り	**約６００通り**

（追加理由）

継続して新たなIoT機器向けのマルウェアが登場していることを踏まえ当該マルウェアで利用されている識別符号や、機器の初期設定の識別符号等を新たに調査対象とするため。

(2) 特定アクセス行為の送信元のIPアドレスの追加

変更前	変更後
４１アドレス	**５４アドレス**

（追加理由）

(1)により入力する識別符号が増加することから、特定アクセス行為に係る通信量も増加し通信回線を増設するため

5Gの本格開始に伴うセキュリティ対策の強化

5Gのセキュリティについて、セキュリティ・バイ・デザインの観点から、総合的な対応を推進。

①脆弱性の検証手法や体制の確立

- 5Gのネットワークに関する脆弱性（ソフトウェア含む）を明らかにするための技術的検証を実施。また、ハードウェアの脆弱性（チップの脆弱性）を発見するための手法に関する技術的検証を実施。
- 脆弱性検出技術の成果を活用（技術移転を含む）し、関連する脅威の分析の視点を踏まえた5Gシステムや利用者に対するインパクト分析を実施し、必要なセキュリティ対策に反映。
- 上記の検証・分析の取組に関し、5Gの事業者・運用者やベンダー、研究機関等が協力して実施する体制を確立。

※Beyond 5Gを見据えた技術開発も促進。

②脆弱性の情報共有の促進

- （一社）ICT-ISACの「5Gセキュリティ推進グループ」において、事業者・運用者間で5Gのリスク情報や脅威情報などの共有を推進。

③対策の促進

規制的措置

- サプライチェーンリスク対応を含む十分なサイバーセキュリティ対策を講じることを全国5Gの開設計画の認定及びローカル5Gの免許の条件とし、対策の実施状況について定期的にフォローアップ。

振興的措置

- 全国５G及びローカル５Gの導入事業者に対する税制優遇措置等により、安全・安心な５Gシステムの普及を支援。

Beyond 5G 推進戦略（全体像）

- **Beyond 5G推進戦略**は、
  ①2030年代に期待されるInclusive、Sustainable、Dependableな社会を目指した**Society 5.0実現のための取組**。
  ②Society 5.0からバックキャストして行う**コロナに対する緊急対応策**かつ**コロナ後の成長戦略を見据えた対応策**。
- 本戦略に基づく**先行的取組**については、大阪・関西万博が開催される**2025年をマイルストーンとして世界に示す**。

基本方針

グローバル・ファースト

- **国内市場をグローバル市場の一部と捉える**とともに、**我が国に世界から人材等が集まるようにする**といった双方向性も目指す。

ｲﾉﾍﾞｰｼｮﾝを生むｴｺｼｽﾃﾑの構築

- **多様なプレイヤーによる自由でアジャイルな取組**を積極的に促す制度設計が基本。

リソースの集中的投入

- 我が国のプレイヤーが**グローバルな協働に効果的に参画**できるようになるために必要性の高い施策へ一定期間集中的にリソースを投

政府と民間が一丸となって、国際連携の下で戦略的に取り組む

研究開発戦略

先端技術への集中投資と、
大胆な電波開放等による

世界最高レベルの研究開発環境の実現

2025年頃から順次要素技術を確立

知財・標準化戦略

戦略的オープン化・デファクト化の促進と、海外の戦略的パートナーとの連携等による

ゲームチェンジの実現

（サプライチェーンリスクの低減と市場参入機会の創出）

Beyond 5G必須特許シェア10%以上

展開戦略

5G・光ファイバ網の社会全体への展開と、5Gソリューションの実証を通じた産業・公的利用の促進等による

Beyond 5G readyな環境の実現

2030年度に44兆円の付加価値創出

Beyond 5Gの早期かつ円滑な導入

Beyond 5Gにおける国際競争力強化

インフラ市場シェア3割程度
デバイス・ソリューション市場でも持続的プレゼンス

産学官の連携により強力かつ積極的に推進

Beyond 5G推進コンソーシアム

①各戦略に基づき実施される具体的な取組の共有、②国内外の企業・大学等による実証プロジェクトの立ち上げ支援、③国際会議の開催

※総務省の部局横断的タスクフォースが戦略の進捗を管理。

テレワークにおけるセキュリティ対策の強化

- 総務省では従来から「**テレワークセキュリティガイドライン**」を**策定**し、**セキュリティ対策の考え方**を示している。
- 新型コロナウイルスの影響により、これまで未導入だった中小企業等においてもテレワークの導入が広まる中で、**実践的かつ具体的で分かりやすい内容のチェックリスト**を作成し、2020年９月に公表。
- またチェックリスト策定と併せ、**セキュリティ対策**に関する**実態調査**と**専門的な相談対応**を実施中。

チェックリストの策定

テレワークセキュリティガイドライン

（2018年４月　第４版）

2004年12月初版
2006年４月第２版
2013年３月第３版

【想定読者像】

- ✓ システム管理者のほか経営層や利用者を幅広く対象
- ✓ 専門の担当や部門が存在
- ✓ 基本的なIT用語は仕組みとして理解しているレベル
- ✓ 基本的なシステム設定作業は、補助解説なく実施可能

2020年度内に改定予定

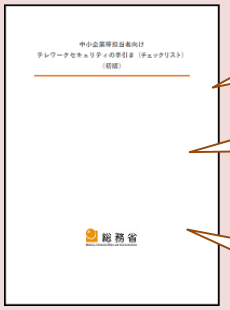
追加

中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)

（2020年９月　初版）

【想定読者像】

- ✓ システム管理担当者向け
- ✓ 専任の担当・部門は存在しない
- ✓ 基本的なIT用語は聞いたことがあるレベル
- ✓ 基本的なシステム設定作業は検索しながら実施可能



テレワーク方式を特定し、その方式に**対応するチェックリストを確認**

チェックリストは**最低限のセキュリティを確実に確保**してもらうためのものに限定

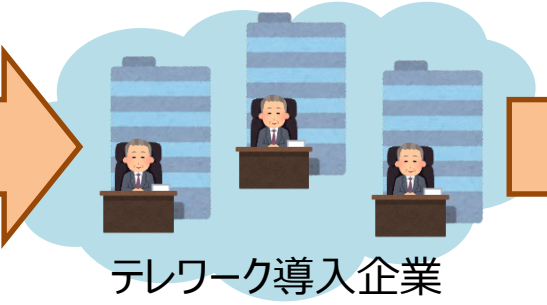
テレワーク用ソフトについて、**設定解説資料を作成**し具体的設定を解説

2020年内を目途に実態調査の結果等を踏まえて改定予定

公表先

実態調査／専門相談対応

テレワーク導入企業が拡大しており、セキュリティ等の実態や課題について調査
（結果はチェックリスト策定にもフィードバック）



テレワーク導入企業

相談申込先

テレワーク導入時・導入後における
セキュリティ対策の専門的な相談

https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

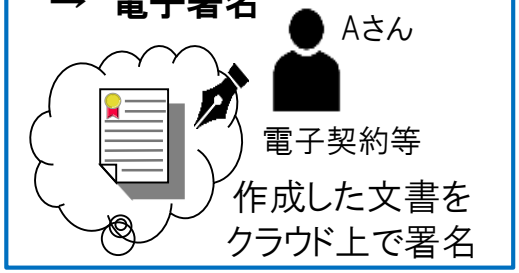
トラストサービスとは

■ データの自由な流通（Data Free Flow with Trust）は、これからの成長のエンジン。

■ Society5.0の実現に向けて、サイバー空間と実空間の一体化が進展し、社会全体のデジタル化を進める中、その有効性を担保する基盤として、ネット利用者の本人確認やデータの改ざん防止等の仕組みである**トラストサービス**が必要。

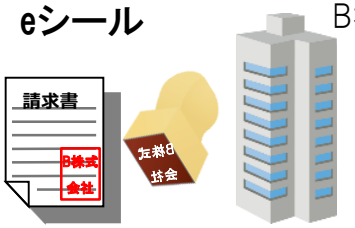
国の制度（電子署名法）有り

①意思を確認
→ 電子署名



制度無し

②文書の起源を確認
→ eシール



組織が発行する文書

民間の認定スキーム有り

④データの存在証明
→ タイムスタンプ

制度無し

③データの送信元（モノ）の正当性を確認

IoT機器（センサー等）から
発せられるデータ

制度無し

⑤データの送達等の保証（①～④の組合せによるサービス）

トラストサービスにより期待される効果の例

① 電子署名のクラウド利用への適用（リモート署名※）により、ICカード携行が不要となり、**テレワークや出張の際でも、速やかに電子契約が締結可能となることで、ビジネスの迅速化に寄与**

※ 利用者がサーバにリモートでログインし、サーバ上で行う電子署名のこと

② 文書の起源を簡便に確認できることにより、企業の文書等の電子化を推進し、**社内業務や企業間取引を効率化**

③ ビッグデータの発信元である**IoT機器等からのデータの真正性を確保し、なりすましを防止**

④ いつ作成された電子データであるか保証されることで、**電子データのみで長期保存が可能となり文書の保存コストが低減**

⑤ **トラストサービスを活用した新たなサービスの創出**
（例：”書留”の電子版）

トラストサービス検討WG取りまとめ

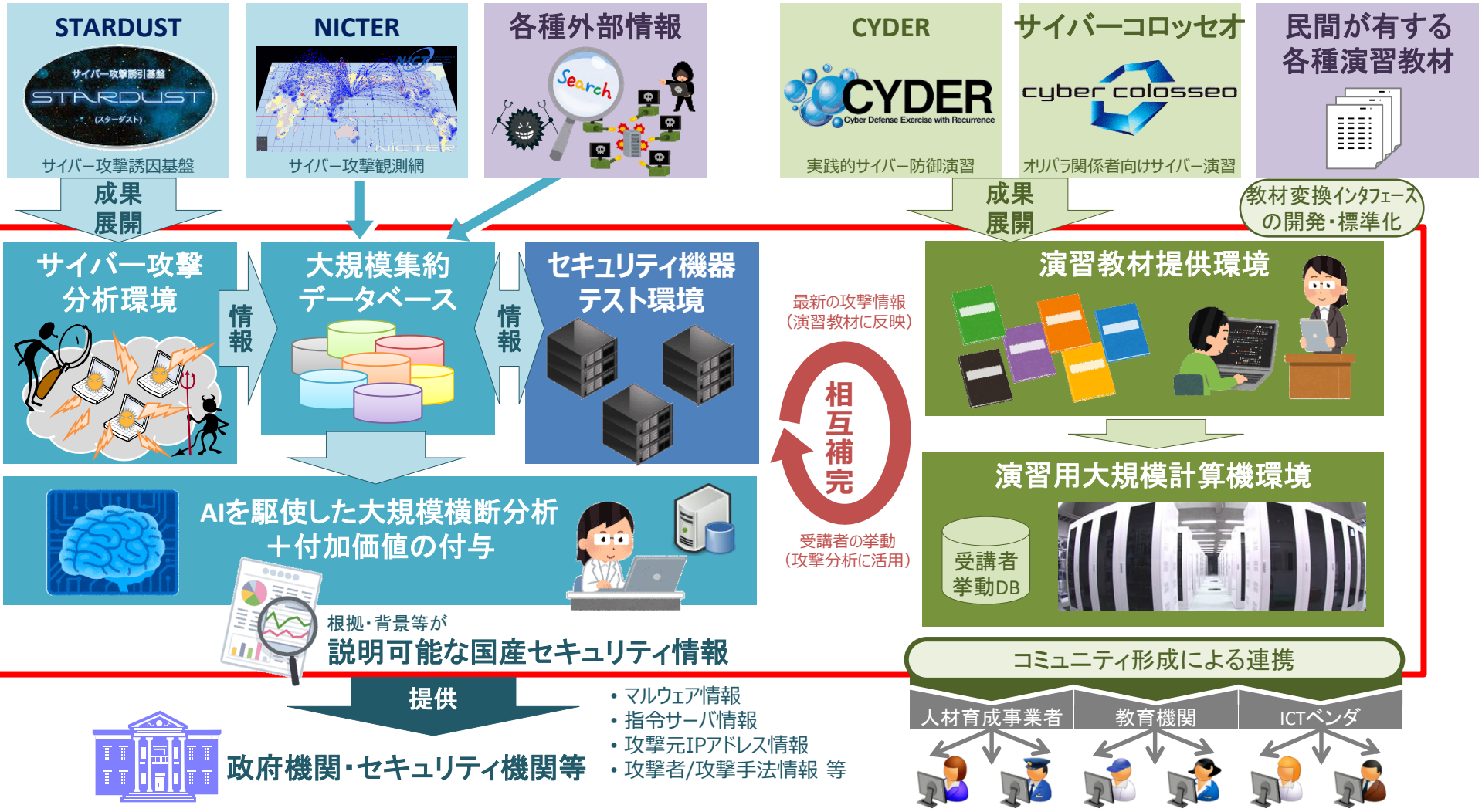
■ 具体的なニーズと課題が顕在化しているタイムスタンプ、eシール、リモート署名について取組の方向性を提示。

現状・課題	取組の方向性
〇データの存在証明の仕組み（タイムスタンプ） • **民間の認定スキームの下で、一部の分野を除き、利用が十分に広がっていない**。 → 電子データと紙による保存を併存している実態があり、保存コストを要している。	• タイムスタンプ事業者に対する**国としての認定制度を創設**。
〇文書の起源を確認できる仕組み（eシール） • 請求書や領収書等について、企業が電子的に発行したことを**簡便に保証する仕組みがない**。 → 企業内の業務や企業間の取引における**電子化が進まず、業務効率化の妨げ**となっている。	• 企業間の書類のやり取りの現状を把握しつつ、**eシールが有効なユースケースについて、幅広く検討。**
〇意思を確認できる仕組み（電子署名） • クラウドを活用した**リモート署名など最新の技術に制度が十分に対応しきれていない**部分が存在。 → 電子署名の利用が伸びていない。 • リモート環境で本人だけが安全に署名できるための**技術的な要件について民間団体で検討中**。	• リモート署名の**電子署名法上の位置づけについて検討**。

■ 上記に加え、電子文書の送受信・保存について規定している**法令との関係で有効な手段として認められるトラストサービスの要件を明示するよう、所管省庁への働きかけ**を行う。

サイバーセキュリティ統合知的・人材育成基盤の構築

■ サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を情報通信研究機構（NICT）に構築し、産学の結節点として開放することで、サイバーセキュリティ対応能力の向上を図る。



総務省のサイバーセキュリティ分野における国際連携の取組について

■ 総務省では、サイバーセキュリティに関する二国間・多国間の連携や対ASEAN諸国を中心とする能力構築支援の取組を実施するとともに、ISACやISP間の国際連携を推進している。

①二国間・多国間連携

総務省のサイバーセキュリティ政策について、積極的な対外発信と連携強化を実施。

・二国間連携
- インターネットエコノミーに関する日米政策協力対話
- 日EU・ICT政策対話・戦略ワークショップ
- その他、豪、中韓、英、仏を含む13か国等とのサイバー協議　等

・多国間連携
- OECD SDE
- ITU-T SG17
- 日・ASEANサイバーセキュリティ政策会議　等

＊　イスラエルとの連携
2018年11月、国家サイバー総局との間でサイバーセキュリティ分野における協力覚書を締結。

②民間組織の国際連携の推進

・ISP向け日ASEAN情報セキュリティワークショップ

日本とASEAN各国のISP事業者等との情報共有等の推進

・日米ISAC連携ワークショップ

日米の情報通信分野ISAC(*)間における情報共有の推進。ICT-ISACと米国IT-ISACとは2019年11月に協力覚書を締結。

ICT-ISACと米国IT-ISACによる覚書署式の様子（2019年11月）

(*) ISACとは、Information Sharing and Analysis Center（情報共有分析センター）の略で、サイバー攻撃のインシデント情報等を収集・分析し、業界内で共有することを目的として、事業分野ごとに設立される組織。

③能力構築支援

・日ASEANサイバーセキュリティ能力構築センター(AJCCBC)

日・ASEAN統合基金（JAIF）を活用したASEAN域内のセキュリティ人材育成（４年間で700人程度を育成する目標）の拠点となるセンターで、2018年９月にタイで開所。ASEAN域内で高い評価を得ている。

■ 研修プログラムの概要

1. サイバーセキュリティ演習

政府機関や重要インフラ事業者等に対し、実践的サイバー防御演習（CYDER）等のプログラムを実施（年6回程度）

2. Cyber SEA Game

若手技術者・学生がサイバー攻撃対処能力を競う大会の開催（年１回）　※いずれも現在オンライン化を推進中。

・世界銀行との連携

マルチ基金「DDP（Digital Development Partnership）」による途上国への能力構築支援を実施。

■主なプロジェクト

1．第1回Cybersecurity Study Tour in Tokyo
ASEAN諸国及び南アジア政府関係者向けのスタディツアー

2．第2回Cybersecurity Study Tour in Tokyo
ASEAN諸国及びインド政府関係者向けのスタディツアー

3．西アフリカ諸国経済共同体向けワークショップへの参画

ASEAN諸国との連携におけるNICTERの活用

■ JASPER。2013年9月の「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議」の共同閣僚声明にて、ネットワークセキュリティ分野における技術協力を強化するため、日・ASEAN間のプロジェクトとして開始。「サイバー攻撃予知即応プロジェクト（PRACTICE ）」及び「感染警告（DAEDALUS）」の総称。

JASPER（ジャスパー）
（**J**apan-**A**SEAN **S**ecurity **P**artn**ER**ship）

○Japan-ASEAN Security PartnERshipの略。
○「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議」の共同閣僚声明にて、ネットワークセキュリティ分野における技術協力を強化するため、日・ASEAN間のプロジェクトとして開始。「サイバー攻撃予知即応プロジェクト（PRACTICE）」及び「感染警告（DAEDALUS）」の総称。

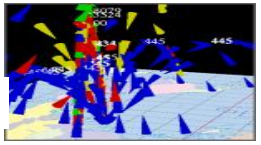
サイバー攻撃予知即応プロジェクト（PRACTICE（プラクティス） ）

○Proactive Response Against Cyber-attacks Through International Collaborative Exchangeの略。
○サイバー攻撃に関する情報を収集・分析の上、情報共有を行い、サイバー攻撃発生の予知・即応を可能とする技術を確立するための研究開発プロジェクト。総務省予算15億円規模で、H23年度からH27年度に実施された。PRACTICEにて設置したセンサーを通じて、現状も一部の国よりサイバー攻撃観測データの提供を受けている。

感染警告（DAEDALUS（ダイダロス））

○Direct Alert Environment for Darknet And Livenet Unified Securityの略。
○独立行政法人情報通信研究機構（NICT）による、マルウェア感染をリアルタイムに警告するサービス。
（2012年6月に国内でサービスを開始）

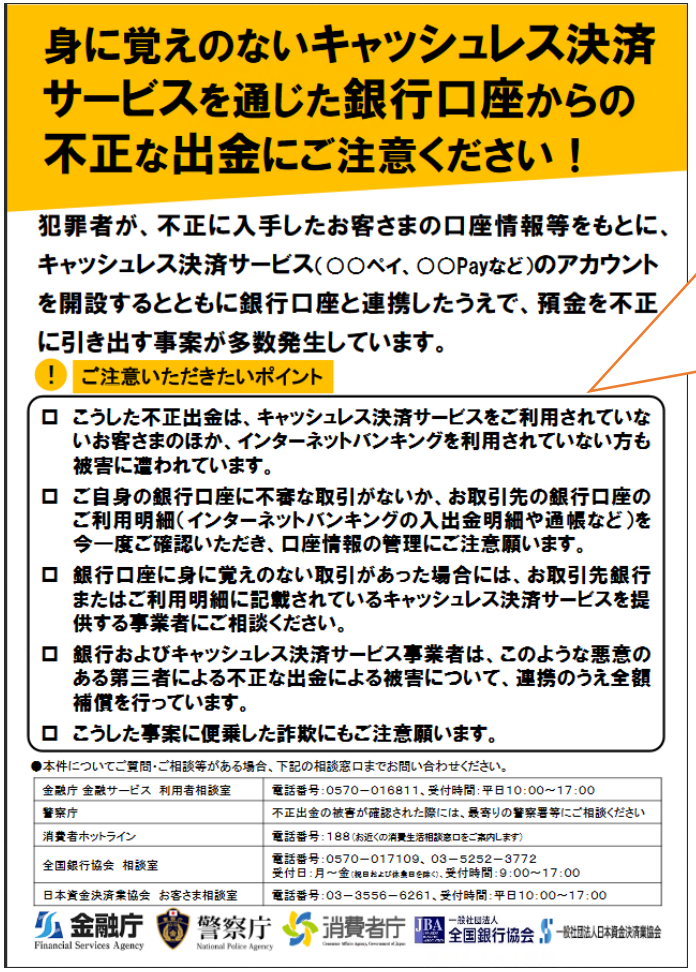
NICTER（ニクター）



○Network Incident analysis Center for Tactical Emergency Responseの略。
○独立行政法人情報通信研究機構（NICT）による、ネットワーク上のサイバー攻撃をリアルタイムに観測・分析するシステム。
○NICTERによる実証結果を、PRACTICEにおいて新たな技術の確立に反映。
○NICTERによる分析結果を活用して、感染警告（DAEDALUS）を実施。

他省庁におけるユーザに対する周知啓発事例

■ 本年10月、警察庁・金融庁等が、身に覚えのないキャッシュレス決済サービスを通じて銀行口座から不正に出金される手口に関する注意喚起を実施。



身に覚えのないキャッシュレス決済サービスを通じた銀行口座からの不正な出金にご注意ください！

犯罪者が、不正に入手したお客さまの口座情報等をもとに、キャッシュレス決済サービス（○○ペイ、○○Payなど）のアカウントを開設するとともに銀行口座と連携したうえで、預金を不正に引き出す事案が多数発生しています。

！ ご注意いただきたいポイント

- こうした不正出金は、キャッシュレス決済サービスをご利用されていないお客さまのほか、インターネットバンキングを利用されていない方も被害に遭われています。
- ご自身の銀行口座に不審な取引がないか、お取引先の銀行口座のご利用明細（インターネットバンキングの入出金明細や通帳など）を今一度ご確認いただき、口座情報の管理にご注意願います。
- 銀行口座に身に覚えのない取引があった場合には、お取引先銀行またはご利用明細に記載されているキャッシュレス決済サービスを提供する事業者にご相談ください。
- 銀行およびキャッシュレス決済サービス事業者は、このような悪意のある第三者による不正な出金による被害について、連携のうえ全額補償を行っています。
- こうした事案に便乗した詐欺にもご注意願います。

●本件についてご質問・ご相談等がある場合、下記の相談窓口までお問い合わせください。

金融庁 金融サービス 利用者相談室	電話番号：0570−016811、受付時間：平日10:00〜17:00
警察庁	不正出金の被害が確認された際には、最寄りの警察署等にご相談ください
消費者ホットライン	電話番号：188（お近くの消費生活相談窓口をご案内します）
全国銀行協会 相談室	電話番号：0570−017109、03−5252−3772 受付日：月〜金（祝日および休業日を除く）、受付時間：9:00〜17:00
日本資金決済業協会 お客さま相談室	電話番号：03−3556−6261、受付時間：平日10:00〜17:00

金融庁 Financial Services Agency　警察庁 National Police Agency　消費者庁　一般社団法人全国銀行協会　一般社団法人日本資金決済業協会

- こうした不正出金は、キャッシュレス決済サービスをご利用されていないお客さまのほか、インターネットバンキングを利用されていない方も被害に遭われています。
- ご自身の銀行口座に不審な取引がないか、お取引先の銀行口座のご利用明細（インターネットバンキングの入出金明細や通帳など）を今一度ご確認いただき、口座情報の管理にご注意願います。
- 銀行口座に身に覚えのない取引があった場合には、お取引先銀行またはご利用明細に記載されているキャッシュレス決済サービスを提供する事業者にご相談ください。
- 銀行およびキャッシュレス決済サービス事業者は、このような悪意のある第三者による不正な出金による被害について、連携のうえ全額補償を行っています。
- こうした事案に便乗した詐欺にもご注意願います。

加えて、警察庁ウェブサイトにおいては、各種サービスに係るアカウント情報（ID・パスワード等）が犯罪等に悪用されることがないよう、以下の事項についても注意喚起。

- 他のサービス等で使用していない、かつ、推測されづらい十分な強度を有するパスワードを設定する。
- ２段階認証・２要素認証等の追加的な認証機能があれば、積極的に利用する。
- パスワード等のアカウント情報は他人に知られないよう、厳重に管理する。
- 自身が利用するサービスを提供する事業者等からの連絡等により、自身のアカウント情報が流出等した疑いが生じた場合には、パスワード（暗証番号等を含む。）を変更してください。
- なお、そのような連絡等を装ったフィッシング等の被害に遭わないよう、正規の事業者からの連絡等であるか慎重に確認してください。